This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of encryption, of a digital signal processor, comprising:

preprocessing, in said digital signal processor, an ~~said~~ input message wherein said preprocessing includes a permutation of said input message;

partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix;

computing a determinant of said matrix;

public key encrypting said determinant; and

multiplying said matrix by said encrypted determinant.

2. (Canceled)

3. (Previously Amended) The method of claim 1, wherein:

said permutation of claim 1 is generated by a hash of said input message.

4. (Currently Amended) The method of claim 1~~2~~, wherein:

said permutation of claim 1 is generated by a random sequence.

5. (Previously Amended) The method of claim 1, wherein:

said preprocessing of claim 1 comprises exclusive ORing said message after permutation with generators of said permutation.

6. (Previously Amended) The method of claim 1, wherein:

said encrypting of claim 1 is public-key encryption.

7. (Previously Amended) The method of claim 6, wherein:

said public-key encryption is RSA.

8. (Previously Amended) The method of claim 1, wherein:

said partitioning of claim 1 first fills the principal diagonal of said matrix.

9. (Currently Amended) A method of encryption of ~~for~~ a digital signal processor, comprising:

preprocessing, in said digital signal processor, an ~~said~~ input message wherein said preprocessing includes a permutation of said input message and defining a permutation source partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix;

generating a permuted message for said ~~an~~ input message employing said permutation source;

padding said permuted message with said permutation source to obtain a preprocessed message; and

encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message.

10. (Previously Amended) The method of claim 9, wherein:

said permutation source is generated by a hash of said input message.

11. (Previously Amended) The method of claim 9, wherein:

said permutation source is generated by a random sequence.

12. (Previously Amended) The method of claim 9, wherein:

said block-based encryption is a public key encryption.

13. (Currently Amended) A method of decrypting, of a digital signal processor, comprising:

Computing, in said digital signal processor, a determinant of a matrix-based encrypted message matrix, wherein said encrypted message was generated by partitioning an input message into matrix elements, wherein said matrix is a square matrix and wherein said matrix encrypted message had preprocessing by a permutation and by applying the inverse of a ~~said~~ permutation to the results;

private key decrypting of said determinant; and

multiplying said matrix by the results of said decrypting.

14. (Canceled)

15. (Previously added) The method of claim 9, wherein said padding includes prepending said permuted message with said permutation source to obtain said preprocessed message.

16. (Previously added) The method of claim 9, wherein said padding includes appending said permuted message with said permutation source to obtain said preprocessed message.